MILBERG TADLER PHILLIPS GROSSMAN LLP
David Azar
(dazar@milberg.com)
11766 Wilshire Blvd, Suite 500
Los Angeles, CA 90025
(212) 594-5300
Facsimile: (212) 868-1229

Ariana J. Tadler (pro hac to be filed)
(atadler@milberg.com)
Henry J. Kelston (pro hac to be filed)
(hkelston@milberg.com)
One Pennsylvania Plaza, Suite 1920
New York, NY 10119
(212) 594-5300
Facsimile: (212) 868-1229

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

KATHI MCGUIRE, individually and on behalf of all others similarly situated, Plaintiff, v. FACEBOOK, INC., Defendant.	CASE NO. **CLASS ACTION** COMPLAINT FOR: 1. Breach of Implied Contract 2. Negligence 3. Violation of California Business and Professions Code § 17500 *et seq.*; JURY TRIAL DEMANDED

Plaintiff Kathi McGuire brings this Class Action Complaint against Facebook Inc. ("Facebook" or "Defendant") on behalf of herself and all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

SUMMARY OF THE ALLEGATIONS

1. Facebook is the world's largest social networking website, with more than two billion monthly active users as of June 2017. Facebook operates a social networking website that allows people to communicate with their family, friends, and coworkers by sharing (or "posting") information, including text, photographs, website links, and videos. Facebook is also widely used by companies and organizations to advertise and promote their products and causes.

2. To establish a Facebook account you are required to share your name, gender, date of birth, and your email address or mobile phone number. After that, Facebook tracks and stores any personally identifiable information users add to their accounts, including schools, maiden name, hometown, current city, employment, and group affiliations such as political clubs, and alumni associations; every IP address from which the user logs in; every friend in the network, including deleted friends; all of the user's activity on Facebook – ever. That includes every post, every "like," every status change, and every search for another person on Facebook.[1]

3. Some users' accounts also contain credit or debit card information.

4. All of this information is "Personally Identifiable Information" or "PII", which is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

5. The collection of massive amounts of PII is central to Facebook's business model. Most of Facebook's revenues, which exceeded $40 billion in 2017, were from the sale of targeted advertising; that is, advertising delivered to Facebook users selected on the basis of the PII the company maintains about them.

[1] Kirsten Korosec, *This Is the Personal Data that Facebook Collects—And Sometimes Sells*, Fortune (Oct. 4, 2018), http://fortune.com/2018/03/21/facebook-personal-data-cambridge-analytica/.

6. On September 28, 2018, Facebook disclosed that a breach of the company's computer network resulted in hackers obtaining direct access to the accounts of 50 million Facebook users and all of the information accessible in and through those accounts (the "Data Breach"). In addition, once they had access to the users' Facebook accounts, "the attackers could have gained access to apps like Spotify, Instagram and hundreds of others that give users a way to log into their systems through Facebook."[2]

7. Plaintiff brings this class action against Facebook for its failure to secure its users' PII, and for its misrepresentations and omissions in its public statements about its information-security practices.

PARTIES

8. Plaintiff Kathi McGuire ("McGuire") is a resident and citizen of California. Plaintiff McGuire opened a Facebook account prior to July 2017. On September 28, 2018, Plaintiff McGuire received a notification from Facebook that her account and PII may have been compromised.

9. Defendant Facebook is a Delaware Corporation that maintains its headquarters in Menlo Park, California. Facebook conducts its business throughout California, the nation, and internationally. Facebook's securities trade on the NASDAQ under the ticker symbol "FB."

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over the state law claims pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the amount in controversy exceeds $5,000,000 exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizens of astate different from that of Defendant. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

[2] Mike Isaac and Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. Times (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

11. Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391 as Defendant is a corporation that does business in and is subject to personal jurisdiction in this District. Defendant's headquarters are located within this District. A substantial part of the acts or omissions at issue in this action occurred in this District. In addition, Facebook's terms of service governing users provides that any claim, cause of action, or dispute must be filed "exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County" and, further, that "[t]he laws of the State of California will govern . . . any claim that might arise" between Facebook and its users.

CHOICE OF LAW

12. Facebook's terms of service provide, in relevant part:

> For any claim, cause of action, or dispute you have against us that arises out of or relates to these Terms or the Facebook Products ("claim"), you agree that it will be resolved exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County. You also agree to submit to the personal jurisdiction of either of these courts for the purpose of litigating any such claim, and that the laws of the State of California will govern these Terms and any claim, without regard to conflict of law provisions.

13. In accordance with the choice of law provision, California common law and statutory law applies to all claims by Facebook users.

FACTUAL BACKGROUND

A. Facebook's Entire Business Model Depends On The Collection And Storage Of Massive Amounts Of PII .

14. In 2017, Facebook's annual revenue was $40.65 billion.

15. Most of Facebook's revenue comes from the sale of targeted advertising; that is, advertising delivered to selected users based on the extensive data Facebook collects and maintains about its users. Accordingly, Facebook's business model is based on the collection, analysis, and monetization of PII.

> The social media giant uses a lot of what it knows about you to show you ads it thinks you might like, and advertisers pay Facebook to plug their products to the right customers. It's called targeted ads, and it's almost the entire way that company keeps the lights on; nearly all of its $40 billion revenue comes specifically from targeted ads. Facebook doesn't technically sell your data to outsiders, it sells access to you based on your data.[3]

16. Recode, a respected technology news website, explains:

> Facebook collects a lot of data about you — everything from your email address to the strength of your phone's battery. The simplest explanation for this is that Facebook uses that data to make money. No, Facebook doesn't sell your data. But it does sell access to you, or more specifically, access to your News Feed, and uses that data to show you specific ads it thinks you're likely to enjoy or click on. This targeted advertising is big business for Facebook. The company reported advertising revenue of $40 billion last year, and it's only going to keep growing.[4]

17. In 2016, in an article titled "98 personal data points that Facebook uses to target ads to you," the Washington Post noted: "While you're logged onto Facebook, for instance, the network can see virtually every other website you visit. *Even when you're logged off*, Facebook knows much of your browsing: It's alerted every time you load a page with a "Like" or "share" button, or an advertisement sourced from its Atlas network." (Emphasis added.)

18. According to Peter Eckersley, the chief computer scientist at the Electronic Frontier Foundation, Facebook's targeting methods are "the most invasive in the world." Eckersley says: "[N]o company on earth, save Facebook, bundles all that information."[5]

---

[3] Grace Lisa Scott, *How Does Facebook Make Money? Here Are 4 Big Ways*, Inverse (May 10, 2018), https://www.inverse.com/article/44566-how-does-facebook-make-money-mark-zuckerberg

[4] Kurt Wagner, *This is How Facebook Uses Your Data for Ad Targeting*, Recode (Apr. 11, 2018, 6:00 AM), https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg.

[5] Caitlin Dewey, *98 personal data points that Facebook uses to target ads to you*, Wash. Post (Aug. 19, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?noredirect=on&utm_term=.8d14d7fdb905

19. When Facebook CEO Mark Zuckerberg testified before Congress in April 2018, Representative Ben Luján asked Zuckerberg "how many data points the social network collects on each user, citing reports that it could be up to 29,000. The 33-year-old executive's answered that he didn't know."[6]

B. Facebook Collects Massive Amounts of Personal and Biographical Data.

20. According to Facebook itself, the PII the company collects includes:

- "the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others . This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our camera"
- information users provide about their work, education, health, religious vies, political views, places they have lived, their relationship status, family members, and dates of birth and other significant life events.
- "information about the people, Pages, accounts, hashtags and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history)[.]
- information about "the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera."[7]

21. Facebook also "receive[s] and analyze[s] content, communications and information that other people provide" about users, "such as when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information."[8]

C. Facebook Collects Credit And Debit Card Numbers And Other Account Information.

---

[6] Rob Price, *Mark Zuckerberg says Facebook collects data on non-users for 'security' – here's the whole story*, Business Insider (Apr. 11, 2018, 3:26 PM), https://www.businessinsider.com/mark-zuckerberg-facebook-collects-data-non-users-for-security-2018-4

[7] Facebook Data Policy, https://www.facebook.com/about/privacy (last visited Oct. 9, 2018).

[8] *Id.*

22. Facebook's terms of service state:

> If you use our Products for purchases or other financial transactions (such as when you make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details

D. Facebook Collects Detailed Device Information.

23. Facebook "collect[s] information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products," including:

- Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
- Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- Data from device settings: information you allow us to receive through device settings you turn on, such as access to your GPS location, camera or photos.
- information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you stream a video from your phone to your TV.
- Cookie data: data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy and Instagram Cookies Policy.

E. Users Rely On Facebook's PII Security Practices

24. Facebook maintains a privacy policy: available on its website ("Privacy Policy"). Facebook's Privacy Policy states, *inter alia*:

> **We design privacy into our products from the outset**
>
> We design privacy into Facebook products with guidance from experts in areas like data protection and privacy law, security, interface design, engineering, product management, and public policy. Our privacy team works to build these diverse perspectives into every stage of product development.
>
> **We work hard to keep your information secure**
>
> We work around the clock to help protect people's accounts, and we build security into every Facebook product. Our security systems run millions of times per second to help catch threats automatically and remove them before they ever reach you. You can also use our security tools like two-factor authentication to help keep your account even more secure.
>
> **You own and can delete your information**
>
> You own the information you share on Facebook. This means you decide what you share and who you share it with on Facebook, and you can change your mind. That's why we give you tools for deleting anything you've posted. We remove it from your timeline and from our servers. You can also delete your account whenever you want.

Facebook's Privacy Principles, https://www.facebook.com/about/basics/privacy-principles (last visited Oct. 9, 2018).

25. Users place value in data privacy and security, and they consider it when making decisions regarding their online behavior. Plaintiff would not have provided the same types and amounts of PII to Facebook had she known that Facebook does not take reasonable and necessary precautions to secure the information.

26. Facebook has repeatedly stated that"[e]veryone has the right to expect strong protections for their information," thus acknowledging that its users place a high value on data privacy and security and, further, that users rely on Facebook's representations about the security it provides. In fact, Facebook made that statement 120 times in its written responses to questions from the Energy and Commerce Committee of the U.S. House of Representatives submitted on June 29, 2018.

27. Contrary to its representations, Facebook failed to maintain reasonable and adequate data security, thereby allowing the Data Breach affecting at least 50 million users.

28. Facebook failed to disclose its negligent and insufficient data security practices and users relied on or were misled by this omission into using Facebook and/or into providing PII to Facebook that they would not otherwise have provided..

29. Facebook is no stranger to threats against its users' PII. In 2013, Facebook disclosed a software flaw that exposed 6 million users' phone numbers and email addresses to unauthorized viewers for a year, while a technical glitch in 2008 revealed confidential birthdates on 80 million Facebook users' profiles. In 2018, 50 million Facebook profiles were harvested for Cambridge Analytica and allowed unauthorized people to control 50 million accounts.

30. Likewise, the technology industry is rife with similar examples of hackers targeting users' PII, including the hacks at Equifax and Yahoo, among many others, all of which pre-date the time-frame Facebook has identified regarding the Data Breach here. According to Statista, there were 169 million records exposed in 2015 – more than double the number exposed in 2014 (85,610,000), many of them pertaining to the compromise of PII.[9]

F. Facebook's Inadequate Security Practices Permitted Attackers To Breach 50 Million User Accounts

31. On September 28, 2018, Facebook announced that the PII of 50 million users had been exposed as a result of the largest data breach in the company's history.

[9] Statista, https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide (last visited Oct. 9, 2018).

32. Facebook alerted users that a security issue was discovered on September 25, 2018. Hours after the announcement, it became evident that the breach exposed not only the information in users' Facebook accounts, but also the users' information in thousands of other applications and services as well. The breach resulted from attackers exploiting a feature called "View As," which allows users to see their Facebook pages as someone else would, a feature initially created to give users more control over their privacy. The attackers exploited Facebook's "View As" code to gain access to user accounts and potentially take control of them by stealing digital keys that permitted access to users' accounts, known as access tokens.

33. Control of the access tokens permit attackers to log in to user accounts without the need for a password, thereby allowing the hackers to take over the accounts and use them exactly as if they were the account holders. That would include changing permissions and privacy settings, and posting or viewing information shared by any of that account's friends.

34. These access tokens could have also been used to access user accounts with third-party companies that use Facebook's "Login with Facebook" function. The "Login with Facebook" function provides users with a faster, more convenient way of signing in to third-party websites and services using their Facebook credentials rather than needing to create countless new usernames and passwords for every website and service.

35. There are tens of thousands of websites and services, such as apps, online retailer sites, and games, for which Facebook users routinely use the "Login with Facebook" function. These include some of the most popular services on the internet, including Instagram and WhatsApp (both owned by Facebook), Uber, eBay, Linked In, Tindr, Airbnb, Netflix, Trip Advisor, Yelp, Spotify, Pinterest, and Pandora.

36. The Data Breach may, in fact, affect 90 million or more users, as the vulnerability in the "View As" feature exposed access tokens not just for the accounts directly hacked but also for users who were the subject of a "View As" inquiry:

> That means that, if Alice used the View As feature to see what her profile would look like to Bob, then Bob's account might have been compromised in this attack.... This morning, in addition to resetting the access tokens

> and thus logging out the 50 million accounts that Facebook knows were affected, Facebook has also reset access tokens for another 40 million that been the subject of any View As look-up in the past year."[10]

G. Stolen PII Is Valuable To Hackers And Thieves

37. It is well known, and the subject of many media reports, that PII data is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto, is well known, as noted above. Despite well-publicized litigation and frequent public announcements of data breaches by some of the world's largest companies, Facebook opted to maintain an insufficient and inadequate system to protect the PII of Plaintiff and class members.

38. Legitimate organizations and the criminal underground alike recognize the value of PII. Otherwise, they wouldn't aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million users, they also took registration data from 38 million users."[11] Similarly, the 2017 Equifax data breach resulted in the compromise of records containing the PII of at least 145.5 million users in the United States and nearly 1 million users outside of the United States.

39. One measure of the economic value of the information exposed in the Data Breach is the price on the "dark web" (*i.e.,* the "black market") for login credentials for Facebook accounts and the other accounts to which the hackers may have gained access. According to one source, Facebook logins sell for $5.20 per account.[12] Credit card details, which may be accessible in some users' Facebook accounts, sell for $50 each; debit card details sell for $67.50.[13]

---

[10] Electronic Freedom Foundation, https://www.eff.org/deeplinks/2018/09/facebook-data-breach-affects-least-50-million-users (last visited Oct. 9, 2018).

[11] Verizon 2014 Payment Card Industry ("PCI") Compliance Report, https://www.verizonenterprise.com/resources/reports/rp_pci-report-2014_en_xg.pdf , at 54 (last visited Oct. 9, 2018) ("2014 Verizon Report").

[12] Simon Migliano, *Dark Web Market Price Index (US Edition)*, https://www.top10vpn.com/privacy-central/privacy/dark-web-market-price-index-feb-2018-us/ (last visited Oct. 2, 2018).

[13] *Id.*

40. Other types of accounts that can be accessed using "Login with Facebook" include eBay, Uber, and Airbnb. A hacker who obtains access to the Facebook account of a user who logs into these services through "Login with Facebook" obtains access to the user's accounts on those services. On the dark web, eBay logins are valued at $12.48 each; Uber logins at $7.00 each; Airbnb logins at $7.87 each.

41. Biographical data is also highly sought after by data thieves. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[14] PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of theft and unauthorized access have been the subject of many media reports. One form of identity theft, branded "synthetic identity theft," occurs when thieves create new identities by combining real and fake identifying information and then use those identities to open new accounts. "This is where they'll take your Social Security number, my name and address, someone else's birthday and they will combine them into the equivalent of a bionic person," said Adam Levin, Chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft, experts say: "It's tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person." In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number.

42. Unfortunately, and as is alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of third parties, such as technology companies, Facebook's approach at maintaining the privacy of Plaintiff and Class members' PII was plainly negligent.

H. This Data Breach Will Result In Additional Identity Theft And Identity Fraud

43. Facebook failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII it collected and retained.

[14] 2014 Verizon Report, at 54.

44. The ramifications of Facebook's failure to keep Plaintiff's and Class members' data secure are severe.

45. Identity thieves can use PII such as that of Plaintiff and Class members to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Among other forms of fraud, identity thieves may get medical services using users' compromised PII or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

46. While Facebook has invalidated 90 million users' single sign-on access tokens following the September 28, 2018 breach (invalidating the compromised 50 million user accounts as well as 40 million more that used the "View As" feature exploited by attackers), researchers warn that most access token hijacking victims still lack any reliable "single sign-off" capabilities that will revoke attackers' access to hyper-connected web services and mobile apps.[15]

I. Annual Monetary Losses From Identity Theft Are In The Billions Of Dollars.

47. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from

[15] Mathew J. Schwartz, *Facebook Breach: Single Sign-On of Doom*, Data Breach Today (Oct. 2, 2018), http://www.databreachtoday.com/blogs/facebook-breach-single-sign-on-doom-p-2668

> data breaches cannot necessarily rule out all future harm.[16]

48. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages.

J. Plaintiff And Class Members Suffered Damages

49. The Data Breach was a direct and proximate result of Facebook's failure to properly safeguard and protect Plaintiff and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Facebook's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

50. Plaintiff's and Class members' PII is private and sensitive in nature and was left inadequately protected by Facebook. Facebook did not obtain Plaintiff's and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

51. As a direct and proximate result of Facebook's wrongful action and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud.

52. Facebook's wrongful actions and inaction directly and proximately caused the theft of Plaintiff and Class members' PII, causing them to suffer actual harm for which they are entitled to compensation, including:

a. theft of their PII;

[16] GAO, *Report to Congressional Requesters*, at p.33 (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Oct. 9, 2018).

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by the misuse of their PII;

c. the improper disclosure of their PII;

d. loss of privacy;

e. ascertainable losses in the form of the value of their PII, for which there is a well-established market; and

f. PII deprivation of rights they possess under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200).[17]

53. While the PII of Plaintiff and members of the Class has been stolen, the same or a copy of the PII continues to be held by Facebook. Plaintiff and members of the Class have an undeniable interest in ensuring that this information is secure, remains secure, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

54. Plaintiff seeks relief in her individual capacity and as a representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of:

All persons in the United States who registered for Facebook accounts and whose PII was compromised as a result of the Data Breach disclosed on September 28, 2018.

55. Excluded from each of the above Classes are Facebook, including any entity in which Facebook has a controlling interest, is a parent or subsidiary, or which is controlled by Facebook, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Facebook. Also excluded are the judges and court personnel in this case and any members of their immediate families.

56. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is

[17] *See also, e.g.,* GAO, August 2018 Data Protection Actions Taken By Equifax and Federal Agencies in Response to the 2017 Breach, https://www.gao.gov/assets/700/694158.pdf

unknown to Plaintiff at this time, Facebook has acknowledged that the accounts of 50 million users was affected by the breach, including Plaintiff's.

57. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Facebook violated the California's Unfair Competition Law by failing to implement reasonable security procedures and practices;

b. Whether class members may obtain injunctive relief against Facebook under California's privacy laws to require that it safeguard the PII of Plaintiff and Class members;

c. Which security procedures and which data-breach notification procedures should Facebook be required to implement as part of any injunctive relief ordered by the Court;

d. Whether Facebook has an implied contractual obligation to use reasonable security measures;

e. Whether Facebook has complied with any implied contractual obligation to use reasonable security measures;

f. What security measures, if any, must be implemented by Facebook to comply with its implied contractual obligations;

g. Whether Facebook violated California's privacy laws in connection with the actions described here; and

h. What the nature of the relief should be, including equitable relief, to which Plaintiff and the Class members are entitled.

58. All members of the proposed Classes are readily ascertainable. Facebook has access to addresses and other contact information for millions of members of the Classes, which can be used for providing notice to many Class members.

59. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other class member, was inadequately safeguarded through Facebook's uniform misconduct.

60. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

61. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

62. Pursuant to Fed. R. Civ. P. 23(c)(4), Plaintiff and the class seek certification of particular claims and issues in the alternative to certification of all issues and claims.

63. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Facebook's violations of law inflicting substantial damages in the aggregate would go un-remedied.

64. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Facebook has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I

Breach of Implied Contract

(On Behalf of Plaintiff and the Class)

65. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 64.

66. Facebook solicited and invited Plaintiff and Class Members to use its services. Plaintiff and Class members accepted Facebook's offers and created user accounts requiring the provision of PII with Facebook during the period of the Data Breach.

67. When Plaintiff and Class Members used Facebook services and products, they provided their PII. In so doing, Plaintiff and Class Members entered into implied contracts with Facebook pursuant to which Facebook agreed to safeguard and protect such information.

68. Each use of a Facebook service or product made by Plaintiff and Class Members was made pursuant to the mutually agreed-upon implied contract with Facebook under which Facebook agreed to safeguard and protect Plaintiff and Class Members' PII.

69. Plaintiff and Class Members would not have provided and entrusted their PII to Facebook in the absence of the implied contract between them and Facebook.

70. Plaintiff and Class Members fully performed their obligations under the implied contracts with Facebook.

71. Facebook breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the PII of Plaintiff and Class.

72. As a direct and proximate result of Facebook's breaches of the implied contracts between Facebook and Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail above

COUNT II

Negligence

(On Behalf of Plaintiff and the Class)

73. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 64.

74. Upon accepting and storing Plaintiff and Class Members' PII in its computer network, Facebook undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Facebook knew, acknowledged, and agreed that the PII was private and

confidential and would be protected as private and confidential. In addition, Cal. Civ. Code § 1798.81.5 requires Facebook to take reasonable methods of safeguarding the personal information of Plaintiff and the Class.

75. Facebook knew that Plaintiff and the class members' PII was personal and sensitive information.

76. Facebook breached its duty to Plaintiff and the Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured personal PII. Furthering its dilatory practices, Facebook failed to provide adequate supervision and oversight of the PII with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiff's and Class Members' PII, misuse the PII, and intentionally disclose it to others without consent.

77. Through Facebook's acts and omissions described in this Complaint, including Facebook's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Facebook unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff and Class Members' PII during the time it was within Facebook's possession or control.

78. Upon information and belief, Facebook improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

79. Facebook's failure to take proper security measures to protect Plaintiff and Class Members' sensitive PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff and Class Members' PII.

80. Facebook's conduct was negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct adequate regular security audits, and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' PII.

81. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

82. As a direct and proximate cause of Facebook's conduct, Plaintiff and the Class suffered damages as alleged above.

COUNT III

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code § 17200 — Unlawful Business Practices

(On Behalf of Plaintiff and the Class)

83. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 64.

84. Facebook has violated Cal. Bus. and Prof. Code §17200 et seq. by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200.

85. Facebook engaged in unlawful acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' personal and sensitive PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Facebook to take reasonable methods of safeguarding the personal information of Plaintiff and the Class.

86. Facebook knew or should have known that its computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data breach or theft was highly likely. Facebook's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

87. Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq.*, including, but not limited to, restitution to Plaintiff and the Class of money or property that Facebook may have acquired by means of its unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Facebook because of its unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

COUNT IV

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code § 17200 — Unfair Business Practices

(On Behalf of Plaintiff and the Class)

88. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 64.

89. Facebook engaged in unfair acts and practices with respect to its services by establishing the sub-standard security practices and procedures described here; by soliciting and collecting Plaintiff and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the Class. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the Class outweighed their utility, if any.

90. As a direct and proximate result of Facebook's acts of unfair practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

91. Facebook knew or should have known that its computer systems and data security practices were inadequate to safeguard the Class Members' PII and that the risk of a data breach or theft was highly likely. Facebook's actions in engaging in the above-named unlawful practices

and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

92. Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq.*, including, but not limited to, restitution to Plaintiff and the Class of money or property that the Facebook may have acquired by means of its unfair business practices, restitutionary disgorgement of all profits accruing to Facebook because of its unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT V

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code § 17200 — Fraudulent/Deceptive Business Practices

(On Behalf of Plaintiff and the Class)

93. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 64.

94. Facebook engaged in fraudulent and deceptive acts and practices with regard to the its services provided to the Class by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII from unauthorized disclosure, release, data breaches, and theft; and representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' PII. These representations were likely to deceive members of the public, including Plaintiff and the Class Members, into believing their PII was securely stored, when it was not, and that Facebook was complying with relevant law, when it was not.

95. Facebook engaged in fraudulent and deceptive acts and practices with regard to the services provided to the Class by omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Class Members' PII. At the time that Class members were using Facebook's services, Facebook failed to disclose to Class Members

that its data security systems failed to meet legal and industry standards for the protection of their PII. These representations were likely to deceive members of the public, including Plaintiff and the Class, into believing their PII was securely stored, when it was not, and that Facebook was complying with relevant law and industry standards, when it was not.

96. As a direct and proximate result of Facebook's deceptive practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

97. Facebook knew or should have known that its computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data breach or theft was highly likely. Facebook's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

98. Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq.*, including, but not limited to, restitution to Plaintiff and the Class of money or property that the Facebook may have acquired by means of its fraudulent and deceptive business practices, restitutionary disgorgement of all profits accruing to Facebook because of its fraudulent and deceptive business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Facebook as follows:

A. For an Order certifying the Class as defined here, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Facebook from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff and Class members'

PII, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class members;

C. For equitable relief compelling Facebook to utilize appropriate methods and policies with respect to user data collection, storage, and safety and to disclose with specificity to Class members the type of PII compromised.

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Facebook's wrongful conduct;

E. For an award of actual damages and compensatory damages, in an amount to be determined;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial of his claims by jury to the extent authorized by law.

DATED: October 9, 2018

s/ David Azar

MILBERG TADLER PHILLIPS GROSSMAN LLP
David Azar
11766 Wilshire Blvd, Suite 500
Los Angeles, CA 90025
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

MILBERG TADLER PHILLIPS GROSSMAN LLP
Ariana J. Tadler
Henry J. Kelston
Jennifer Czeisler
One Pennsylvania Plaza, Suite 1920
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229